REMARKS/ARGUMENTS

Reexamination and reconsideration of this application as amended is requested. By this amendment, Claims 1, 4, 6, 7, 9-11, 13, 19-21, and 27, have been amended, and Claims 15-18 and 23-26 have been canceled, and new Claim 28 has been added. After this amendment, Claims 1-14, 19-22, and 27-28 remain pending in this application.

Claim Rejection under 35 U.S.C. § 112, second paragraph

(1-3) The Examiner rejected Claim 4, under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as the invention.

Applicants have amended Claim 4 to more clearly recite "the executable external module". The term "the executable external module" in Claim 4 now recites in proper antecedent basis. Additionally, Applicants amended independent Claim 1 to more clearly recite "an executable external module" which is also in proper antecedent form. Support for the term "executable external module" is found in the original specification as filed. For example, see page 5, lines 7-18. Note that with the untampered external module the application executes normally. No new matter was added by this amendment.

In view of these amendments to Claims 1 and 4, and the remarks above, Applicants believe that the rejection of Claim 4 under 35 U.S.C. § 112, second paragraph, as discussed above, has been overcome. Applicants kindly request that the Examiner withdraw the rejection of Claim 4.

Claim Rejections - 35 USC § 103

(4-15) The Examiner rejected Claims 1-2, 4-5, 7-9, 10-13, 21, and 27, under 35 U.S.C. 103(a) as being unpatentable over Moore (U.S. Patent 5,343,527) in view of Brown et al. (U.S. Patent 4,972,472).

Applicants have amended independent Claims 1, 13, and 27, and amended dependent Claims 4, 7, 9, 10, 11, and 21, to more clearly, and in proper antecedent form, recite the present invention. These amendments were made to correct antecedent basis and not to add any limitation or for patentability in view of any cited prior art reference. Additionally, independent Claims 1, 13, 21, and 27, were further amended to more clearly and distinctly recite the present invention. Note in particular that the STOMPing and the UNSTOMPing, e.g., the disrupting of the executable external module rendering it unusable and the restoring of the executable external module to a usable state, are performed at the same computer system. Additionally, new Claim 28 recites that the disrupting and the restoring are performed at run time of the executable external module at the computer system. Support for the amended claim language is found in the original patent application as filed. For example, see the specification, on page 5, lines 7-13, and on page 7, lines 20-24, and on page 8, lines 5-11. Note in particular page 7, lines 20-21, discussing the exemplary embodiment and stating that "K gets recreated at run time in two different ways". No new matter was added by these amendments to the claims.

Moore's scheme is essentially a combined encryption and digital signature of a software module. Under Moore, a *publisher* encrypts and signs a protected software module during the publishing process using a private key. This makes the module *unusable* for all entities that are not implementing Moore's scheme. At *runtime*, and typically at a subscribing computer system that is different than the publisher, the public key is retrieved, the signature is validated and, if the module is authentic, the decryption step is performed.

This is fundamentally different than what is accomplished according to the presently claimed invention. It is an objective of Moore's method to *make the protected software unusable* to anyone who is not participating in the publishing and subscription system. This is problematic, as identified by our patent application. See, for example, page 4, lines 17 – 24 of our application. On the other hand, the presently claimed invention leaves *the protected executable external module intact* such that any applications that are not aware of the inventive authentication scheme can still use the executable external module even though they are not able to validate the module's authenticity. According to the presently claimed methods and system, as recited for all the independent claims, and for the dependent claims depending therefrom, respectively, both the STOMP and the UNSTOMP steps are performed at the same computer system, and as recited in certain dependent claims including new claim 28, these steps are performed at *run time* of the executable external module. Another advantage of the presently claimed invention is that it avoids the single point of failure created by the signature validation step. This is a significant problem that can allow hackers to easily break through security schemes. See page 2, lines 17-23 of our patent application. As a matter of fact, Moore's invention is a good example of the kind of digital signature based technology that our invention improves upon. See, for example, page 4, lines 14-24, of our patent application where we recognized this problem as the state of the prior art. This problem is clearly visible from the signature validation process described by Moore in column 12, lines 41–58. Note that the single point of comparison to determine authenticity is subject to easy hacker attack. Our claimed invention avoids this altogether by performing the STOMP processing and then the UNSTOMP processing of the executable external module to authenticate it for subsequent use by the computer system.

Moore's scheme does not solve the problem being addressed by the presently claimed invention. The initial creation of the data K (Moore, column 9, lines 24 – 47) is part of the *publishing process* and it intentionally leaves the software in an *unusable* state. According to the presently claimed invention, it leaves the software module in a *usable* state while optionally adding the authentication data to the module that remains

usable. This executable external module then can be distributed to a computer system that could validate its authenticity before executing the module, if the computer system is equipped with the present invention, or that would execute the module without authentication if the computer system lacks our present invention. Also, note that Moore's scheme does resolve itself to a yes/no question at runtime at the point where the encrypted hash and the actual hash are compared. This is the single point of failure our inventive STOMP and UNSTOMP method avoids. According to an embodiment of our claimed invention, the disruption caused by the STOMP method happens at *run time,* and then would be *immediately followed* by the UNSTOMP at the same computer system. The protected executable external module remains intact and usable during distribution and the single point of failure is avoided since there is no comparison. These are significant advantages of the presently claimed invention not found in any of the cited prior art.

We would also like to point out that Moore's scheme could not be used to solve the problem we are addressing simply by moving the publishing step into the run time and forgoing the distribution and directory mechanisms. Moore's publishing process (see column 9, lines 24–47), which in the Office Action the Examiner appears to compare to our STOMP process, actually is not suitable for run time use *since it requires a private key*. We observe that in our inventive method, both the STOMP and the UNSTOMP process are performed using public key information. The assumption that Moore's publishing step and our STOMP step are equivalent is plainly wrong.

Also, Moore's preferred embodiment of software to be protected by his invention is *source* code (see column 4, lines 45 – 50). Our claimed invention is directed at executable code or binary modules such as DLL or SO files.

In addition to the arguments above, with respect to the rejection of claims 13, 21, and 27, see page 5 of Office Action, numbered section 15, we would like to point out that the browsing process described by Moore in column 13, lines 40–55, is fundamentally

different than the presently claimed storing of the executable external module or loading the module. Under Moore, the clear text metadata associated with the encrypted software package is loaded and browsed. In our presently claimed invention, the module itself is loaded and/or stored in memory. There is no need to manage metadata separately because, unlike Moore, our invention does not require the external module to be invalidated (e.g., be unusable) while it is distributed. The examiner also refers to column 12, lines 27 – 40, in Moore's patent in relationship with our Claim 13. However column 12, lines 27 – 40, in Moore's patent describes the signature validation process. There is no similarity at all with the STOMP process as recited for our Claim 13. The same applies to our Claims 21 and 27.

To summarize, as discussed above, Moore's scheme addresses a different problem and does NOT solve the problem that our claimed invention solves. Moore's approach was clearly recognized by our patent application as the state of the prior art which our claimed invention improves upon.

Lastly, it should also be clear that the teachings of the cited Brown reference, being directed to a method for changing a master key in a cryptographic system, do not address the problem or in any way teach or suggest the solution as recited for the presently claimed invention.

Accordingly, in view of the amendments and remarks above, since neither Moore, Brown, nor any combination of the two cited references, teaches, anticipates, or suggests, the presently claimed invention, Applicants believe that the rejection of Claims 1-2, 4-5, 7-9, 10-13, 21, and 27under 35 U.S.C. 103(a) has been overcome. The Examiner should withdraw the rejection of these claims. Further, Applicants believe that new Claim 28, depending from amended independent Claim 1, also recites in allowable form, and the Applicants kindly urge the Examiner to also allow this new claim.

(16-17) The Examiner rejected Claim 8, under 35 U.S.C. 103(a) as being unpatentable over Moore (U.S. Patent 5,343,527) in view of Brown et al. (U.S. Patent 4,972,472), and further in view of Ghizzo et al. (U.S. Patent 6,698,016).

Applicants have amended independent Claim 1 to more clearly and distinctly recite the presently claimed invention. Dependent claim 8 depends from Claim 1 and therefore recites all of the limitations in Claim 1.

As we have pointed out, Moore and Brown are not relevant to the problem solved by our presently claimed invention. There is no need for Moore or Brown to perform any kind of embedding since Moore transforms the entire protected software package and makes it unusable (see Moore, column 9, lines 44–64). An implementation of Moore's invention is free to add information to the encrypted package in a header or trailer. Our invention, on the other hand, aims to leave the protected module unchanged such that it remains usable (i.e., executable) for applications that are not aware of our invention. Therefore, our inventive approach adds information to the module *without* affecting it's usability by another application. As Claim 8 points out, this can be accomplished by adding an additional section to a PE file. This has the advantage that the authentication token can travel with the protected module - without affecting it's usability. Ghizoni's method is different since it involves injection of code into a module that is part of a process in memory. In our Claim 8, we refer to the process of extending a PE File (a regular Windows DLL module) on disk with an additional piece of data without disrupting the structural integrity of the file.

Ghizzoni teaches us in column 7, line 54, to column 8, line 30, how to use a PE file in order to retrieve the starting address of a process. This is not related to, or relevant for, the use of an additional data section in order to embed an authentication token, as we describe in our Claim 8. Figure 3 in Ghizzoni's patent shows the purpose of retrieving the starting address – to perform a temporary redirection of the control flow. Again,

there is no relevance to our claimed use of an additional section in the PE file in order to store the authentication token without impacting the validity of the module.

Accordingly, in view of the amendments and remarks above, it should be clear that neither Moore, Brown, Ghizzoni, nor any combination of the three cited references, teaches, anticipates, or suggests, the presently claimed invention, as recited for Claim 8. Applicants believe that the rejection of Claim 8 under 35 U.S.C. 103(a) has been overcome. The Examiner should withdraw the rejection of this claim.

(18-19) The Examiner rejected Claims 15 and 23, under 35 U.S.C. 103(a) as being unpatentable over Moore (U.S. Patent 5,343,527) in view of Brown et al. (U.S. Patent 4,972,472), and further in view of Granger et al. (U.S. Patent 6,480,959).

Applicants have canceled dependent Claims 15 and 23 without prejudice, and incorporated their respective limitations into their respective independent Claims 13 and 21.

Again the basis for the rejection hinges on the assumption that the combination of Moore and Brown teach a valid solution to the problem addressed by our claimed invention. As we have already pointed out above, that is not the case.

Granger, in column 10, lines 22-29, refers to XOR as a *potential* encryption algorithm. We use XOR to transform the module during the STOMP and UNSTOMP operations. There is no further similarity and the purpose of Granger's invention is different from the presently claimed invention.

Accordingly, in view of the amendments and remarks above, since neither Moore, Brown, Granger, nor any combination of the three cited references, teaches, anticipates, or suggests, the presently claimed invention, and since Claims 15 and 23 have been canceled, Applicants believe that the rejection of Claims 15 and 23 under 35 U.S.C. 103(a) has been

overcome, and that the respective independent Claims 13 and 21 are also allowable over the three cited references or any combination thereof. The Examiner should withdraw the rejection of these claim.

(20-25) The Examiner rejected Claims 3, 13-14, 16-19, 22, and 24-26, under 35 U.S.C. 103(a) as being unpatentable over Moore (U.S. Patent 5,343,527) in view of Brown et al. (U.S. Patent 4,972,472), and further in view of Granger et al. (U.S. Patent 6,480,959), as applied to Claims 15 and 23, and furthermore in view of Dwork et al. (U.S. Patent 5,978,482).

Applicants have canceled dependent Claims 16-18 and 23-26 without prejudice, and incorporated their respective limitations into their respective independent Claims 13 and 21.

Again the patent examiner's argument hinges on the assumption that Moore and Brown are a valid solution to the problem addressed by our invention. The patent office keeps adding other building blocks: XOR (from Granger) and now Signets (from Dwork). As we have pointed out before, the base patent (Moore) set out to solve a very different problem. Therefore the combination of patents listed by the examiner does NOT in any way solve the problem our invention is designed to solve.

With respect to the teachings of the Dwork patent, first of all, we reference the signet work done by Dwork in our teachings in the present patent application. We would like to point out that one of the co-inventors of the Dwork patent is Mr. Jeff Lotspiech who is also a co-inventor of the present patent application. The teachings in the present patent application significantly extend beyond Dwork's teachings such as to perform non-disruptive authentication of executable external software modules, which is not taught, anticipated, or suggested, by Dwork, or by any of the cited prior art references.

Also, with respect to the arguments presented in the rejection of Claims 3, 16, and 24, on page 7 of the Office Action, in the passage referenced by the Examiner (Moore, column 12, line 46), Moore teaches that the second hash be compared with the first hash and that decryption only occurs if there is a match. This is what we recognized as the state of the prior art (see page 4, line 14 of our patent application) and what we avoid by our STOMP and UNSTOMP processing.

Further, with respect to the arguments presented in the rejection of Claims 14 and 22, on page 7 of the Office Action, again the suggestion that Moore's publishing step (column 10, lines 1–15) is an alternative to our inventive STOMP method is plainly incorrect. We note that our STOMPing of a module such as at run time and immediately before the UNSTOMPing of the module is very different from the Moore publishing step. Moore's publishing step uses a private key which is not available to all applications such as at run time. Moore clearly says so (see column 10, line 7). Clearly, Moore's publishing step is not an alternative to our presently claimed STOMPing process.

Accordingly, in view of the amendments and remarks above, since neither Moore, Brown, Granger, Dwork, nor any combination of the four cited references, teaches, anticipates, or suggests, the presently claimed invention, and since dependent Claims 16-18 and 23-26 have been canceled, Applicants believe that the rejection of 3, 13-14, 16-19, 22, and 24-26, under 35 U.S.C. 103(a) has been overcome, and that the respective independent Claims 1, 13, and 21, are also allowable over the four cited references or any combination thereof. The Examiner should withdraw the rejection of these claim.

(26-27) The Examiner rejected Claim 20 under 35 U.S.C. 103(a) as being unpatentable over Moore (U.S. Patent 5,343,527) in view of Brown et al. (U.S. Patent 4,972,472), and further in view of Granger et al. (U.S. Patent 6,480,959), and further in view of Dwork et al. (U.S. Patent 5,978,482), as applied to Claim 18, and furthermore in view of Golan (U.S. Patent 5,974,549).

This rejection of Claim 20 also is based on the incorrect assumption that Moore and Brown are a valid alternative to the presently claimed invention as recited for independent Claim 13. This incorrect assumption has already been addressed above with respect to the rejection of Claim 13 and the rejection of Claim 18, now canceled.

In addition, the Examiner makes the case that Golan's patent teaches us the use of run time checks to make sure that function calls are not intercepted. Golan indeed teaches us how to intercept API calls and block or allow them in accordance with a given security policy. However, our Claim 20 specifically refers to exactly the opposite situation. The run time checks are designed to *detect interception*, including the process described by Golan, and further to ensure that API calls are actually made only to the authenticated module.

Accordingly, in view of the amendments and remarks above, since neither Moore, Brown, Granger, Dwork, Golan, nor any combination of the five cited references, teaches, anticipates, or suggests, the presently claimed invention, Applicants believe that the rejection of Claim 20 under 35 U.S.C. 103(a) has been overcome, and that the respective independent Claim 13 is also allowable over the five cited references or any combination thereof. The Examiner should withdraw the rejection of this claim.

Conclusion

The foregoing is submitted as full and complete response to the Official Action mailed May 20, 2004, and it is submitted that Claims 1-14, 19-22, and 27-28 are in condition for allowance. Reconsideration of the rejection is requested. Allowance of Claims 1-14, 19-22, and 27-28 is earnestly solicited.

No amendment made was related to the statutory requirements of patentability unless expressly stated herein. No amendment made was for the purpose of narrowing

the scope of any claim, unless Applicants have argued herein that such amendment was made to distinguish over a particular reference or combination of references.

Applicants acknowledge the continuing duty of candor and good faith to disclosure of information known to be material to the examination of this application. In accordance with 37 CFR §§ 1.56, all such information is dutifully made of record. The foreseeable equivalents of any territory surrendered by amendment are limited to the territory taught by the information of record. No other territory afforded by the doctrine of equivalents is knowingly surrendered and everything else is unforeseeable at the time of this amendment by the Applicants and the attorneys.

The present application, after entry of this amendment, comprises twenty (20) claims, including four (4) independent claims. Applicants have previously paid for twenty-seven (27) claims including four (4) independent claims. Applicants, therefore, believe that an additional fee for claims amendment is currently not due.

Additionally, a petition for a two month extension of time to file this Response has been attached to this Response. The Commissioner is hereby authorized to charge the extension fee for response of **($430)**, or if this fee amount is insufficient or incorrect, then the Commissioner is authorized to charge the appropriate fee amount to prevent this application from becoming abandoned, or credit any overpayment, to Deposit Account 50-1556.

If the Examiner believes that there are any informalities that can be corrected by Examiner's amendment, or that in any way it would help expedite the prosecution of the patent application, a telephone call to the undersigned at (561) 989-9811 is respectfully solicited.

The Commissioner is hereby authorized to charge any fees that may be required or credit any overpayment to Deposit Account 50-1556.

In view of the preceding discussion, it is submitted that the claims are in condition for allowance. Reconsideration and re-examination is requested.

Respectfully submitted,

Date: 10/20/04

By: Jose Gutman

Jose Gutman
Reg. No. 35,171

Please send all correspondence concerning this patent application to:

Jose Gutman, Esq.
FLEIT, KAIN, GIBBONS, GUTMAN
BONGINI & BIANCO P.L.
551 N.W. 77th Street, Suite 111
Boca Raton, FL 33487
Tel (561) 989-9811
Fax (561) 989-9812